CLAIMS

1. An apparatus for performing cryptographic operations, comprising:

a cryptographic instruction, received by a computing device as part of an instruction flow executing on said computing device, wherein said cryptographic instruction prescribes one of the cryptographic operations, and wherein said cryptographic instruction prescribes that a user-generated key schedule be employed for execution of said one of the cryptographic operations;

keygen logic, operatively coupled to said cryptographic instruction, configured to direct said computing device to load said user-generated key schedule; and

execution logic, operatively coupled to said keygen logic, configured to employ said user-generated key schedule to execute said one of the cryptographic operations.

2. The apparatus as recited in claim 1, wherein said one of the cryptographic operations further comprises:

an encryption operation, said encryption operation comprising encryption of a plurality of plaintext blocks to generate a corresponding plurality of ciphertext blocks.

3. The apparatus as recited in claim 1, wherein said one of the cryptographic operations further comprises:

a decryption operation, said decryption operation comprising decryption of a plurality of ciphertext blocks to generate a corresponding plurality of plaintext blocks.

4. The apparatus as recited in claim 1, wherein said user-generated key schedule is stored in memory.

5. The apparatus as recited in claim 1, wherein said user-generated key schedule comprises an expanded key schedule according to the Advanced Encryption Standard (AES) algorithm.

6. The apparatus as recited in claim 1, wherein said keygen logic is configured to interpret a key generation field within a control word which is referenced by said cryptographic instruction.

7. The apparatus as recited in claim 1, wherein said cryptographic instruction is prescribed according to the x86 instruction format.

8. The apparatus as recited in claim 1, wherein said cryptographic instruction implicitly references a plurality of registers within said computing device.

9. The apparatus as recited in claim 8, wherein said plurality of registers comprises:

a first register, wherein contents of said first register comprise a first pointer to a first memory address, said first memory address specifying a first location in memory for access of said plurality of input text blocks upon which said one of the cryptographic operations is to be accomplished.

10. The apparatus as recited in claim 8, wherein said plurality of registers comprises:

a second register, wherein contents of said second register comprise a second pointer to a second memory address, said second memory address specifying a second location in said memory for storage of a corresponding plurality of output text blocks, said corresponding plurality of output text blocks being generated as a result of accomplishing said one of the cryptographic operations upon a plurality of input text blocks.

11. The apparatus as recited in claim 8, wherein said plurality of registers comprises:

a third register, wherein contents of said third register indicate a number of text blocks within a plurality of input text blocks.

12. The apparatus as recited in claim 8, wherein said plurality of registers comprises:

a fourth register, wherein contents of said fourth register comprise a third pointer to a third memory address, said third memory address specifying a third location in memory for access of cryptographic key data for use in accomplishing said one of the cryptographic operations.

13. The apparatus as recited in claim 12, wherein said user-generated key schedule comprises said cryptographic key data.

14. The apparatus as recited in claim 8, wherein said plurality of registers comprises:

a fifth register, wherein contents of said fifth register comprise a fourth pointer to a fourth memory address, said fourth memory address specifying a fourth location in memory, said fourth location comprising said initialization vector location, contents of said initialization vector location comprising an initialization vector or initialization vector equivalent for use in accomplishing said one of the cryptographic operations.

15. The apparatus as recited in claim 8, wherein said plurality of registers comprises:

a sixth register, wherein contents of said sixth register comprise a fifth pointer to a fifth memory address, said fifth memory address specifying a fifth location in memory for access of a control word for use in accomplishing said one of the cryptographic operations, wherein said control word prescribes cryptographic parameters for said one of the cryptographic operations, and wherein said control word comprises:

a keygen field, configured to specify that said user-generated key schedule be employed during execution of said one of the cryptographic operations.

16. The apparatus as recited in claim 1, wherein said execution logic comprises:

a cryptography unit, configured execute a plurality of cryptographic rounds on each of said plurality of input text blocks to generate a corresponding each of a plurality of output text blocks, wherein said plurality of cryptographic rounds are prescribed by a control word that is provided to said cryptography unit.

17. An apparatus for performing cryptographic operations, comprising:

a cryptography unit within a device, configured to execute one of the cryptographic operations responsive to receipt of a cryptographic instruction within an instruction flow that prescribes said one of the cryptographic operations, wherein said cryptographic instruction also prescribes that a user-generated key schedule be employed when executing said one of the cryptographic operations; and

keygen logic, operatively coupled to said cryptography unit, configured to direct said device to perform said one of the cryptographic operations and to employ said user-generated key schedule when performing said one of the cryptographic operations.

18. The apparatus as recited in claim 17, wherein said user-generated key schedule is stored in memory.

19. The apparatus as recited in claim 17, wherein said user-generated key schedule comprises an expanded key schedule according to the Advanced Encryption Standard (AES) algorithm.

20. The apparatus as recited in claim 17, wherein said keygen logic is configured to interpret a key generation field within a control word which is referenced by said cryptographic instruction.

21. The apparatus as recited in claim 17, wherein said cryptographic instruction is prescribed according to the x86 instruction format.

22. A method for performing cryptographic operations in a device, the method comprising:

receiving a cryptographic instruction that prescribes employment of a user-generated key schedule during execution of one of a plurality of cryptographic operations; and

employing the user-generated key schedule when executing the one of the cryptographic operations.

23. The method as recited in claim 22, wherein said receiving comprises:

via a field within a control word that is referenced by the cryptographic instruction, specifying employment of the user-generated key schedule.

24. The method as recited in claim 22, wherein said employing comprises:

loading the user-generated key schedule from memory.

25. The method as recited in claim 22, wherein the user-generated key schedule comprises an expanded key schedule according to the Advanced Encryption Standard (AES) algorithm.

26. The method as recited in claim 22, wherein said receiving comprises:

prescribing the cryptographic instruction according to the x86 instruction format.